

CLAIMS

1-16. (cancelled)

17. (previously presented) A network configuration entity comprising:
a processor; and
a memory for storing
an NCE list, said NCE list comprising an indication of each device in the network
that may operate as said network configuration entity,
an SCC list, said SCC list comprising an indication of each device allowed to
participate in said secure network,
a DCC list, said DCC list associated with said one or more rules for interaction
between and among devices and comprising definitions that logically bind a port
on the network configuration entity, to one or more other ports resident in the
secure network, and,
a MAC list, said MAC list comprising an indication of network endpoints from
which management access is acceptable.

18. (cancelled)

19. (previously presented) A switching device comprising:
- a processor; and
 - a memory for storing
 - a list of entities eligible to be a primary network configuration entity, wherein the primary network configuration entity has exclusive control of one or more security functions, one of the entities on said list being a default primary configuration entity and identifiable as such by a pre-defined rule, and
 - a network configuration policy set, said network configuration policy set comprising,
 - zoning information defining members of the logical zones in said physical network, and
 - fabric segmentation information defining management procedures to be implemented in the event that said network switch becomes a member of a segmented portion of the network.
20. (cancelled)
21. (previously presented) A switching device comprising:
- a processor; and
 - a memory for storing
 - a list of entities eligible to be a primary network configuration entity, wherein the primary network configuration entity has exclusive control of one or more security functions, one of the entities on said list being a default primary configuration entity and identifiable as such by a pre-defined rule, and
 - MAC policies, said MAC policies defining logical channels from which a pre-defined set of security or management operations may originate.
- 22–53. (cancelled)

54. (previously presented) A method of securing a network, said method comprising:
controlling the recognition, operation and succession of the network configuration entity by designating an NCE list comprising an indication of each device in the network that may operate as said network configuration entity;
designating a unique name for each devices that may participate in the secure network;
indicating port relationships in said secure network to specifically delineate a list of unique names for ports that any given port may communicate with; and
restricting management access to a pre-defined set of access methods.
55. (previously presented) The network configuration entity of claim 17 wherein the network configuration entity is a switching device.
56. (previously presented) The network switch of claim 19 further wherein the memory further stores MAC policies, said MAC policies defining logical channels from which a pre-defined set of security or management operations may originate.
57. (previously presented) The network switch of claim 19 wherein the one or more security functions comprise specifying devices that may facilitate management-level access to the network.
58. (previously presented) The network switch of claim 19 wherein the one or more security functions comprise providing confidentiality or information security for management information being passed over the network.
59. (previously presented) The network switch of claim 19 wherein the one or more security functions comprise limiting use of logical management access channels.
60. (previously presented) The network switch of claim 19 wherein the one or more security functions comprise specifying what devices or entities are allowed in the network.
61. (previously presented) The network switch of claim 19 wherein the one or more security functions comprise specifying what entities are allowed to access what other entities in

the network.

62. (previously presented) The network switch of claim 19 wherein each entity on the list of entities eligible to be a primary network configuration entity is assigned a level in an authority hierarchy.
63. (previously presented) The network switch of claim 62 wherein only one entity on the list of entities eligible to be a primary network configuration entity is assigned to the highest level of the authority hierarchy.
64. (previously presented) The network switch of claim 62 wherein entities assigned to lower levels of the authority hierarchy have exclusive control of only a subset of the one or more security functions.
65. (previously presented) The network switch of claim 21 wherein the one or more security functions comprise specifying devices that may facilitate management-level access to the network.
66. (previously presented) The network switch of claim 21 wherein the one or more security functions comprise providing confidentiality or information security for management information being passed over the network.
67. (previously presented) The network switch of claim 21 wherein the one or more security functions comprise limiting use of logical management access channels.
68. (previously presented) The network switch of claim 21 wherein the one or more security functions comprise specifying what devices or entities are allowed in the network.
69. (previously presented) The network switch of claim 21 wherein the one or more security functions comprise specifying what entities are allowed to access what other entities in the network.

70. (previously presented) The network switch of claim 21 wherein each entity on the list of entities eligible to be a primary network configuration entity is assigned a level in an authority hierarchy.
71. (previously presented) The network switch of claim 21 wherein only one entity on the list of entities eligible to be a primary network configuration entity is assigned to the highest level of the authority hierarchy.
72. (previously presented) The network switch of claim 21 wherein entities assigned to lower levels of the authority hierarchy have exclusive control of only a subset of the one or more security functions.